Criminal underworld is dropping bitcoin for another cryptocurrency

January 10 2018 09:45 PM

Privacy coins such as monero, designed to avoid tracking, have climbed faster over the past two months as law enforcers adopt software tools to monitor people using bitcoin

0

Bloomberg/Portland

Bitcoin is losing its lustre with some of its earliest and most avid fans – criminals – giving rise to a new breed of virtual currency.

Privacy coins such as monero, designed to avoid tracking, have climbed faster over the past two months as law enforcers adopt software tools to monitor people using bitcoin. A slew of analytic firms such as Chainalysis are getting better at flagging digital hoards linked to crime or money laundering, alerting exchanges and preventing conversion into traditional cash.

The European Union's law-enforcement agency, Europol, raised alarms three months ago, writing in a report that "other cryptocurrencies such as monero, ethereum and Zcash are gaining popularity within the digital underground." Online extortionists, who use ransomware to lock victims' computers until they fork over a payment, have begun demanding those currencies instead. On December 18 hackers attacked up to 190,000 WordPress sites per hour to get them to produce monero, according to security company Wordfence.

For ransomware attacks, monero is now "one of the favourites, if not the favourite," Matt Suiche, founder of Dubai-based security firm Comae Technologies, said in a phone interview.

Monero quadrupled in value to $349 in the final two months of 2017, according to coinmarketcap.com, placing it among a number of upstart coins that rose faster than bitcoin, the world's most valuable digital currency. Bitcoin roughly doubled in the same period, data compiled by Bloomberg show.

In monero's case, criminals are snapping it up because bitcoin's underlying technology can work against

them. Called blockchain, the digital ledger meticulously records which addresses send and receive transactions, including the exact time and amount – great data to use as evidence. Match an address to a crime and then watch the bitcoin universe carefully, and you can see the funds disappear and reappear in other locations.

Sleuths have developed databases and techniques for digesting that information to eventually nab wrongdoers. Say, for example, a coffee shop in Berkeley is known to have a certain bitcoin address, and a wallet used by an extortionist transfers the same amount there every morning at 9am. Police can stop by and make an arrest.

Started in 2014, monero is very different. It encrypts the recipient's address on its blockchain and generates fake addresses to obscure the real sender. It also obscures the amount of the transaction.

The techniques are so potent that software that flags coins suspected of being obtained through crime now tags just about anything converted into or out of monero as high risk, according to Pawel Kuskowski, chief executive officer of Coinfirm, which helps exchanges and other companies avoid tainted money. That compares with only about 10% of bitcoin, he said.

"What we treat 'high risk' is something that's anonymising funds," he said in a phone interview. "How are you going to prove that these funds are not coming from illegal sources?"

Monero is one of many privacy-focused coins, each offering different security features. Its main competitor, Zcash – which isn't known to have a significant criminal following – can offer even better privacy protection. Instead of creating fake addresses to hide senders, it encrypts their true address. That makes it impossible to identify senders by looking for correlations in addresses used in multiple transactions to pinpoint the real one – a vulnerability for monero.

Still, Princeton University researchers recently developed a tool that helps them analyse Zcash transactions at least to some extent – but they haven't been able to crack monero. And Zcash high-security features can't be used on disposable burner phones, a favourite of criminals eager to stay anonymous.

Developers behind monero say they simply created a coin that protects privacy. Most people use it legitimately – they just don't want others to know whether they're buying a coffee or a car, Riccardo Spagni, core developer at monero, said in a phone interview.

"As a community, we certainly don't advocate for monero's use by criminals," Spagni said. "At the same time if you have a decentralised currency, it's not like you can prevent someone from using it. I imagine that monero provides massive advantages for criminals over bitcoin, so they would use monero."

Yet criminals are probably only a fraction of monero's users, according to Lucas Nuzzi, a senior analyst at Digital Asset Research, which provides research to institutional investors.

"As with any disruptive technology, many of the initial use cases revolve around illicit activities," he wrote in an e-mail. But as everyday people grow concerned about privacy and surveillance, "there is utility in these currencies that go beyond just a means of exchange for illicit goods."

North Korean hackers prefer Monero

North Korean hackers are hijacking computers to mine cryptocurrencies as the regime in Pyongyang widens its hunt for cash under tougher international sanctions.

A hacking unit called Andariel seized a server at a South Korean company in the summer of 2017 and used it to mine about 70 Monero coins – worth about $25,000 as of December 29 – according to Kwak Kyoung-ju, who leads a hacking analysis team at the South Korean government-backed Financial Security Institute, says Bloomberg.

The case underscores the increasing appetite from cyber-attackers for digital currencies that are becoming a source of income for the Kim Jong-un regime. North Korea is accelerating its pursuit of cash abroad as the world tightens its stranglehold on its conventional sources of money with sanctions cutting oil supplies and other trade bans.

"Andariel is going after anything that generates cash these days," said Kwak. "Dust gathered over time builds a mountain."

The hackers may have seized other computers to mine cryptocurrencies and appear to prefer Monero

because the currency is more focused on privacy and easier to hide and launder than bitcoin, Kwak said, citing the analysis of the server. Andariel was able to take control of the server undetected by its operator, he said.

A cryptocurrency can be earned if a complex mathematical problem is solved, but it requires high-powered computers that often only corporations can afford. Not every company spends as much on protecting their computers from hackers. Yapian, the owner of bitcoin exchange Youbit, said in December it would close after getting breached.

Like bitcoin, Monero uses a network of miners to verify its trades. But it mixes multiple transactions to make it harder to trace the origin of funds, and adopts "dual-key stealth" addresses that make it difficult to pinpoint recipients.

South Korean investigators are looking at North Korea among their suspects.